Politique de gestions des journaux informatiques dans les établissements d'enseignement supérieur

serge.aumont@cru.fr

La gestion des logs et les établissements

- Des pratiques disparates
- Des questions récurrentes de la part des RSSI parce que l'encadrement juridique est complexe, voir mal défini.
- Un groupe de travail SDS-SUP, mandaté par la CPU, la DGES, DGRI, le HFDS
- Une des missions du SDS sup est de proposer un référentiel de bonne pratique dans le domaine de la SSI. La gestion des logs relève donc de ce champs :
- Le résultat : « Politique de gestions des journaux informatiques »
  http://www.cru.fr/_media/activites/securite/gestiondesjournaux.pdf

Genèse de ce document

- Ce document est encore un document de travail
- Initialement inspiré de la déclaration à la CNIL des logs faite par le CNRS
- Proposition élaborée avec plusieurs RSSI et le réseau naissant des CILs
- Aide précieuse de la CNIL dans le cadre de la convention de collaboration entre la CNIL et la CPU

Le contexte juridique :

- Les universités sont simultanément :
  - Employeurs
  - Editeur
  - Hébergeur de contenus
  - Fournisseur d'accès internet
  - …
- Pour chacun de ses rôles, il existe un environnement juridique spécifique et … des juristes spécialisés

Les intervenants

- Administrateurs
- La chaîne fonctionnelle SSI
  - Correspondant sécurité
  - RSSI
  - AQSSI
  - Fonctionnaire de défense

Gestion des logs : les finalités

- Surveillance de la SSI
- Détection des défaillances et intrusions
- Détection des abus contraires aux lois, aux chartes et au règlement intérieur
- Indices et éléments de preuve pour des enquêtes

Mais aussi

- Monitoring applications et réseau
- Assistance aux utilisateurs
- Indicateur de qualité
- …

Durée de conservation selon finalité

- 3 mois : finalité interne
- 1 an : sur réquisition des autorités « présentées dans les formes légales »

- 2 conténaires pour 2 politiques d'accès
- Pas de spécification de l'implémentation des « conténaires »

Sécurité et intégrité des données

- Les serveurs synchronisés sur un service de temps
  - Rapprochement des logs
  - Détection des manques
- La PSSI prévoie les règles de sécurité pour les fichiers contenant des données personnelles, les logs en particulier
- base d'empreintes ou d'horodatage (suggestion de la DCSSI)
- Possibilité d'exportation anonymisée
- Politique de sauvegarde pour la destruction des logs

Les données journalisées

- Messagerie, forum, listes de diffusion
- Serveurs web internes à l'établissement
- Serveurs web externes
- Les équipements réseaux
- Les applications spécifiques

La messagerie

- Machine d'origine et de destination
- Le « sender », les destinataires
- Tailles, Message-Id
- Données d'authentification (SMTP/AUTH)
- Filtrage anti-virus anti-spam
- Listes de diffusion : décisions des modérateurs

Serveurs web internes

- Journalisation des accès
- Machine d'origine
- URL
- Données d'identification
- Données échangées

Serveurs web externes

2 cas :

- Les personnels (et les étudiants ?)
- Les personnes de passage

- Article L34-1 du code des télécommunications : **pas de journalisation du contenu des communications**
- La mort des proxy ?

Équipements réseaux

Il faut pouvoir répondre à la question « A qui était attribuée cette adresse IP à cette date ? ».

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure ;
- les données d'authentification ;

Détection des usages abusifs

- Exemple : détection de machine hébergeant des serveurs warez ou trafic peer to peer
- Traitements systématiques et non visant une personne ou une catégorie de personnes
- Résultats uniquement pour les administrateurs et la chaine fonctionnelle SSI

Droit d'accès

- Chaque personne concernée peut demander les logs la concernant
- Les demandes sont faites par écrit auprès du directeur de composante
- Les résultats transmis avec vérification de l'identité du destinataire

Informations des utilisateurs

- Information et consultation préalable des instances représentatives des personnels
- Référencer la politique de gestion des journaux informatique dans la charte informatique de l'établissement
- Publicité spécifique lors de l'ouverture de nouveaux services ou lors de l'accueil de nouveaux utilisateurs
- Voir Guide pratique CNIL cybersurveillance

Statut actuel

- Une première version de ce document à été visé par l'ensemble des partenaires du SDS Sup
- La CPU a demandé par courrier à la CNIL une position officielle.

- Le document est appelé à évoluer, mais le formalisme qui l'entoure ne facilitera pas les choses.

Questions ?